# Group Data Protection Policy

# General provisions

## Subject-matter and purpose

Camira Group Holdings Limited (Camira) is required to process personal data that is relevant to its operations.

Camira purposes to process personal data in accordance with this Policy and requires all those working under its control to comply with this Policy.

## Material Scope

This Policy applies to the processing of personal data in the context of Camira's operations in its capacity as a data controller (controller) or a data processor (processor) in the European Union (EU), regardless of whether or not the processing takes place in the EU.

This Policy applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system.

This Policy does not apply to the processing of personal data:

a. in the course of an activity which falls outside the scope of EU law;

b. by a natural person in the course of a purely personal or household activity.

In the context of Camira's operations, the processing of personal data can be carried out:

a. by Camira in its capacity as a controller (CONTROLLER);

b. by Camira in its capacity as a controller, in conjunction with a joint controller (CONTROLLER-Joint Controller);

c. by a joint controller, in conjunction with Camira in its capacity as a controller (Joint Controller-CONTROLLER);

d. by a processor, for and on behalf of Camira in its capacity as a controller (Processor-CONTROLLER);

e. by Camira in its capacity as a processor, for and on behalf of a controller (PROCESSOR-Controller);

f. by a processor, for and on behalf of Camira in its capacity as a processor (Processor-PROCESSOR);

g. by Camira in its capacity as a processor, for and on behalf of a processor (PROCESSOR-Processor).

The obligations set out herein under Controller and processor shall apply respectively.

## Territorial Scope

This Policy applies to the processing of personal data in the context of the activities of Camira, in its capacity as a controller or a processor established in the EU, regardless of whether the processing takes place in the EU or not.

This Policy applies to the processing of personal data of data subjects who are in the EU in the context of the activities of Camira, by a controller or processor not established in the EU, where the processing activities are related to:

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or

b. the monitoring of their behaviour as far as their behaviour takes place within the EU.

This Policy applies to the processing of personal data, in the context of the activities of Camira, by a controller not established in the EU, but in a place where Member State law applies by virtue of public international law.

## Definitions

For the purposes of this Policy, the definitions set out in the the applied EU General Data Protection Regulations (GDPR), and, where applicable, the UK Data Protection Act 2018 (DPA18), apply.

Roles, Responsibilities and Authorities

In addition to others set out herein and elsewhere, this Policy determines the following roles, responsibilities as follows.

## Roles, Responsibilities and Authorities

### Board of Directors

Camira's Board of Directors shall have responsibility and authority to:

- determine and record Camira's obligations and/or requirements for designation of a Data Protection Officer (DPO) on a mandatory or voluntary basis.
- designate and appoint a Data Protection Officer (DPO), or an alternative data governance function, subject to the above determination, on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil its tasks, and maintain its expert knowledge.
- support the data governance function in performing its tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations.
- ensure that the data governance function does not receive any instructions regarding the exercise of those tasks.
- ensure that the data governance function is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
- ensure that the data governance function reports into the highest management level.
- ensure that incumbents of the data governance function are not dismissed nor penalised for performing their tasks.
- ensure that assigned tasks and duties do not result in a conflict of interests.
- perform other tasks and duties as required.

### Data Governance Team

Camira's Data Governance Team shall have responsibility and authority to:

- act as the alternative designated data governance function to a designated Data Protection Officer.
- act as the designated contact for data subjects with regard to all issues related to processing of their personal data and to the exercise of their rights.
- inform and advise Camira and employees who carry out processing of their obligations pursuant to Camira's compliance requirements.
- provide advice where requested as regards the data protection impact assessment (DPIA) and monitor its performance pursuant Camira's requirements set out herein;
- cooperate with supervisory authorities and act as the contact point for supervisory authorities on issues relating to processing, including the prior consultation referred to herein, and to consult, where appropriate, with regard to any other matter.

- in the performance of its tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- remain bound by secrecy or confidentiality concerning the performance of its tasks, in accordance with applicable requirements.
- perform other tasks and duties as required.

### Data Protection Response Team

Camira's Data Protection Response Team shall have responsibility and authority to:

- recognise and address security incidents that are relevant to the context and scope of Camira's operations in accordance with Camira's policies and procedures.
- in the performance of its tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- remain bound by secrecy or confidentiality concerning the performance of its tasks, in accordance with applicable requirements.
- perform other tasks and duties as required.

### Data Compliance Team

Camira's Data Compliance Team shall have responsibility and authority to:

- monitor compliance with applicable requirements and with Camira's policies in relation to the protection of personal
- data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits, in accordance with Camira's policies and procedures.
- in the performance of its tasks, have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.
- remain bound by secrecy or confidentiality concerning the performance of its tasks, in accordance with applicable requirements.
- perform other tasks and duties as required.

# Principles

## Principles relating to processing of personal data

Principles relating to processing of personal data

### Accountability

Camira, in its capacity as a controller, takes responsibility for, and shall ensure that it remains capable of demonstrating compliance with, the following Principles:

### Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject.

### Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes.

### Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

### Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step shall be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

### Storage limitation

Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed.

### Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

## Lawfulness of processing

Camira shall ensure that it remains capable of demonstrating lawful processing of personal data.

### Legitimate basis

Processing is considered lawful only if and to the extent that at least one of the identified permissible legitimate bases of processing applies:

a. Consent: the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b. Contract: processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c. Compliance: processing is necessary for compliance with a legal obligation to which the controller is subject, laid down by EU or Member State law;

d. Vital interest: processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e. Public interest: processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, laid down by EU or Member State law;

f. Legitimate interest: processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. This shall not apply to processing carried out by public authorities in the performance of their tasks.

**Processing for a purpose other than that for which the personal data have been collected**

Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent, or on applicable law constituting a necessary and proportionate safeguarding measure, Camira shall, in its capacity as a controller, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, amongst other things:

a. any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;

b. the context in which the personal data have been collected, in particular regarding the relationship between data subjects and Camira;

c. the nature of the personal data, in particular whether special categories of personal data are processed, or whether personal data related to criminal convictions and offences are processed;

d. the possible consequences of the intended further processing for data subjects;

e. the existence of appropriate safeguards, which may include encryption or pseudonymisation.

## Conditions for consent

Where processing is based on consent, Camira, in its capacity as a controller, shall ensure that it remains capable of demonstrating that the data subject has consented to processing of their personal data.

If the data subject's consent is given in the context of a written declaration which also concerns other matters, the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language. Any part of such a declaration which constitutes an infringement of this Policy shall not be binding.

Camira shall recognise and respect the right of the data subject to withdraw the data subject consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw, as to give, consent.

When assessing whether consent is freely given, Camira shall take utmost account of whether, amongst other things, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract.

The term "information society services" is defined as "any service normally provided for remuneration, at a distance, by electronic means and at the individual request of a recipient of services".

Camira shall not offer such information society services directly to a child.

## Processing of special categories of personal data

This Policy prohibits the processing of special categories of personal data, that is personal data revealing: racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership; and the processing of: genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation; unless at least one of the identified permissible exceptions applies:

a. Explicit consent: the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where EU or Member State law provide that the prohibition referred to in the above paragraph may not be lifted by the data subject;

b. Legally necessary: processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by EU or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

c. Vital interest: processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;

d. Legitimate not-for-profit: processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;

e. Manifestly made public: processing relates to personal data which are manifestly made public by the data subject;

f. Legal or judicial process: processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

g. Substantial public interest: processing is necessary for reasons of substantial public interest, on the basis of EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

h. Health provision: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EU or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3, including circumstances in which it is carried out: (a) by or under the responsibility of a health professional or a social work professional, or (b) by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

i. Public health interest: processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of EU or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

j. Public archiving interest: processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with GDPR Article 89(1) based on EU or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

**Processing of personal data relating to criminal convictions and offences**

This Policy prohibits the processing of personal data relating to criminal convictions and offences or related security measures including personal data relating to:

a. the alleged commission of offences by the data subject, or

b. proceedings for an offence committed or alleged to have been committed by the data subject or the disposal of such proceedings, including sentencing;

unless the processing is demonstrably carried out under the control of official authority or when the processing is authorised by EU or Member State law providing for appropriate safeguards for the rights and freedoms of data subjects.

### Processing which does not require identification

if the purposes for which Camira, in its capacity as a controller, processes personal data do not, or do no longer, require the identification of a data subject by Camira, then Camira is not obliged to maintain, acquire or process additional information in order to identify the data subject for the sole purpose of legal compliance.

Where, in such cases, Camira is able to demonstrate that it is not in a position to identify the data subject, it shall inform the data subject accordingly, if possible.

In such cases, requirements relating to data subject rights, including right of access, right to rectification, right to erasure, right to restriction of processing, notification obligations and right to data portability, shall not apply except where the data subject, for the purpose of exercising data subject rights, provides additional information enabling their identification.

# Rights of the data subject

## Transparency and modalities

### Transparent information, communication and modalities for the exercise of the rights of the data subject

Camira, in its capacity as a controller, shall take appropriate measures to provide information relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

This specifically includes information provided relating to obtaining personal data from the data subject or otherwise and any communication in relation to the exercise of subject rights and personal data breach.

Camira shall provide the information in writing, or by other means, including, where appropriate, by electronic means.

This information shall be provided by a Privacy Notice, a Privacy Policy or equivalent.

When requested by the data subject, Camira may provide the information orally, provided that the identity of the data subject is proven by other means.

Camira shall facilitate the exercise of data subject rights referred to later herein in accordance with its Data Subject Request Response Procedures.

In the cases where processing does not require identification specified above, Camira shall not refuse to act on the request of the data subject for exercising the data subject rights referred to later herein unless Camira demonstrates that it is not in a position to identify the data subject.

Camira shall provide information on action taken on a request of the data subject for exercising the data subject rights referred to later herein to the data subject without undue delay and in any event within one month of receipt of the request.

That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Camira shall inform the data subject of any such extension within one month of receipt of the request, together with the reasons for the delay.

Where the data subject makes the request by electronic means, the information shall be provided by electronic means where possible, unless otherwise requested by the data subject.

If Camira does not take action on the request of the data subject, Camira shall inform the data subject without delay (and at the latest within one month of receipt of the request) of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

Camira shall provide, free of charge, information relating to obtaining personal data from the data subject or otherwise and any communication in relation to the exercise of subject rights and personal data breach.

Where requests from a data subject are manifestly unfounded or excessive, in particular because of their repetitive character, Camira may either:

a. charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or

b. refuse to act on the request.

Camira shall bear the burden of demonstrating the manifestly unfounded or excessive character of the request.

Camira shall produce and publish meaningful guidance about such fees charged.

Without prejudice to requirements relating to processing which does not require identification, where Camira has reasonable doubts concerning the identity of the natural person making the request, Camira may request the provision of additional information necessary to confirm the identity of the data subject.

Camira may provide the information to data subjects relating to obtaining personal data from the data subject or otherwise in combination with standardised icons in order to give in an easily visible, intelligible and clearly legible manner a meaningful overview of the intended processing. Where the icons are presented electronically they shall be machine-readable.

Camira shall recognise and respect the rights of data subjects in accordance with relevant Operating Procedures.

## Information to be provided

### Information to be provided where personal data are collected from the data subject

Where personal data relating to a data subject are collected from the data subject, Camira shall, in its capacity as a controller, at the time when personal data are obtained, provide the data subject with all of the following information:

a. the identity and the contact details of Camira and, where applicable, of Camira's representative;

b. the contact details of the Data Protection Officer (DPO), where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. where the processing is based on legitimate interest (as determined herein earlier), the legitimate interests pursued by Camira, or by a third party;

e. the recipients or categories of recipients of the personal data, if any;

f. where applicable, the fact that Camira intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission and, in the case of transfers subject to appropriate safeguards (including approved binding corporate rules and/or reported compelling legitimate interests), reference to those safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to in the above paragraph, Camira shall, at the time when personal data are obtained, provide the data subject with the following further information necessary to ensure fair and transparent processing:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. the existence of the right to request from Camira access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

c. where the processing is based on consent, or explicit consent (as determined herein earlier), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

d. the right to lodge a complaint with a supervisory authority;

e. whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data;

f. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where Camira, intends to further process the personal data for a purpose other than that for which the personal data were collected, it shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to in the above paragraph.

The above paragraphs shall not apply where and insofar as the data subject already has the information.

**Information to be provided where personal data have not been obtained from the data subject**

Where personal data have not been obtained from the data subject, Camira, in its capacity as a controller, shall provide the data subject with the following information:

a. the identity and the contact details of Camira and, where applicable, of its representative;

b. the contact details of the Data Protection Officer, where applicable;

c. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d. the categories of personal data concerned;

e. the recipients or categories of recipients of the personal data, if any;

f. where applicable, the fact that Camira intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the European Commission and, in the case of transfers subject to appropriate safeguards (including approved binding corporate rules and/or reported compelling legitimate interests), reference to those safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to in the above, Camira shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a. the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b. where the processing is based on legitimate interest (as determined herein earlier) the legitimate interests pursued by Camira, or by a third party;

c. the existence of the right to request from Camira access to and rectification or erasure of personal data or restriction of processing concerning the data subject and to object to processing as well as the right to data portability;

d. where processing is based on consent, or explicit consent (as determined herein earlier), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

e. the right to lodge a complaint with a supervisory authority;

f. from which source the personal data originate, and if applicable, whether it came from publicly accessible sources;

g. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Camira shall, shall provide the information referred to above:

a. within a reasonable period after obtaining the personal data, but at the latest within one month, having regard to the specific circumstances in which the personal data are processed;

b. if the personal data are to be used for communication with the data subject, at the latest at the time of the first communication to that data subject; or

c. if a disclosure to another recipient is envisaged, at the latest when the personal data are first disclosed.

Where Camira intends to further process the personal data for a purpose other than that for which the personal data were obtained, it shall provide the data subject prior to that further processing with information on that other purpose and with any relevant further information as referred to above.

The above paragraphs shall not apply where and insofar as:

a. the data subject already has the information;

b. the provision of such information proves impossible or would involve a disproportionate effort, in particular for processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to appropriate conditions and safeguards or in so far as the obligation referred to in the first paragraph is likely to render impossible or seriously impair the achievement of the objectives of that processing. In such cases Camira shall take appropriate measures to protect the data subject's rights and freedoms and legitimate interests, including making the information publicly available;

c. obtaining or disclosure is expressly laid down by EU or domestic law to which Camira is subject and which provides appropriate measures to protect the data subject's legitimate interests; or

d. where the personal data must remain confidential subject to an obligation of professional secrecy regulated by EU or domestic law, including a statutory obligation of secrecy.

## Right of access by the data subject

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to obtain from Camira confirmation as to whether or not personal data concerning the subject are being processed, and, where that is the case, access to the personal data and the following information:

a. the purposes of the processing;

b. the categories of personal data concerned;

c. the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;

d. where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;

e. the existence of the right to request from Camira rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;

f. the right to lodge a complaint with a supervisory authority;

g. where the personal data are not collected from the data subject, any available information as to their source;

h. the existence of automated decision-making, including profiling, and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Where personal data are transferred to a third country or to an international organisation, Camira shall recognise and respect the right of the data subject to be informed of the required appropriate safeguards relating to the transfer.

Camira shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, Camira may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

The right to obtain a copy referred to in the above paragraph shall not adversely affect the rights and freedoms of others.

Where a data subject makes an access request the information to which the data subject is entitled must be provided in writing without undue delay.

Camira may restrict, wholly or partly, the access rights so conferred to the extent that and for so long as the restriction is, having regard to the fundamental rights and legitimate interests of the data subject, a necessary and proportionate measure to:

a. avoid obstructing an official or legal inquiry, investigation or procedure;

b. avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;

c. protect public security;

d. protect national security;

e. protect the rights and freedoms of others.

Where the access rights of a data subject are restricted, wholly or partly, the controller must inform the data subject in writing without undue delay:

a. that the rights of the data subject have been restricted,

b. of the reasons for the restriction,

c. of the data subject's right to make a request to the supervisory authority,

d. of the data subject's right to lodge a complaint with the supervisory authority,

and

e. of the data subject's right to apply to a court.

(a) and (b) do not apply to the extent that the provision of the information would undermine the purpose of the restriction.

Camira shall:

a. record the reasons for a decision to restrict (whether wholly or partly) the access rights of a data subject, and

b. if requested to do so by the Supervisory authority, make the record available to the Supervisory authority.

## Rectification and erasure

### Right to rectification

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to obtain from Camira without undue delay the rectification of inaccurate personal data concerning the data subject.

Taking into account the purposes of the processing, Camira shall recognise and respect the right of the data subject to have incomplete personal data completed, including by means of providing a supplementary statement.

### Right to erasure ('right to be forgotten')

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to obtain from Camira the erasure of personal data concerning the data subject without undue delay and Camira shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

a. the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b. the data subject withdraws consent on which the processing is based, according to the definitions given above, and where there is no other legal ground for the processing;

c. the data subject exercises their right to object to the processing and there are no overriding legitimate grounds for the processing, or the data subject exercises their right to object to processing of personal data for direct marketing purposes;

d. the personal data have been unlawfully processed;

e. the personal data have to be erased for compliance with a legal obligation in EU or domestic law to which Camira is subject;

f. the personal data have been collected in relation to the offer of information society services referred to above.

Where Camira has made the personal data public and is obliged under the first paragraph to erase the personal data, Camira, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

The above paragraphs shall not apply to the extent that processing is necessary:

a. for exercising the right of freedom of expression and information;

b. for compliance with a legal obligation which requires processing by EU or domestic law to which Camira is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in Camira;

c. for reasons of public interest in the area of public health;

d. for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in so far as the right referred to in the first paragraph is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

e. for the establishment, exercise or defence of legal claims.

**Right to restriction of processing**

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to obtain from Camira restriction of processing where one of the following applies:

a. the accuracy of the personal data is contested by the data subject, for a period enabling Camira to verify the accuracy of the personal data;

b. the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c. Camira no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

d. the data subject has exercised their right to object to processing pending the verification whether the legitimate grounds of Camira override those of the data subject.

Where processing has been restricted under the above paragraph, such personal data shall, with the exception of storage, only be processed by Camira with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the EU or of the United Kingdom.

A data subject who has obtained restriction of processing pursuant to the first paragraph shall be informed by Camira before the restriction of processing is lifted.

**Notification obligation regarding rectification or erasure of personal data or restriction of processing**

Camira, in its capacity as a controller, shall communicate any rectification or erasure of personal data or restriction of processing carried out, in accordance with Camira's policies relating to the subject's rights to rectification, erasure and rectification, to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

Camira shall inform the data subject about those recipients if the data subject requests it.

### Right to data portability

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to receive the personal data concerning the data subject, which the data subject has provided to Camira, in its capacity as controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from Camira to which the personal data have been provided, where:

a. the processing is based on consent, or explicit consent, or on a contract pursuant to the definitions given above; and

b. the processing is carried out by automated means.

In exercising the data subject right to data portability pursuant to the above paragraph, Camira shall recognise and respect the right of the data subject to have the personal data transmitted directly from one controller to another, where technically feasible.

The exercise of the right referred to the first paragraph shall be without prejudice to the right to erasure. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in Camira.

The right referred to in the first paragraph shall not adversely affect the rights and freedoms of others.

## Right to object and automated individual decision making

### Right to object

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject to object, on grounds relating to the data subject particular situation, at any time to processing of personal data concerning the data subject which is based on the legal bases of public interest or legitimate interest as define above, including profiling based on those provisions.

Camira shall no longer process the personal data unless it demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

Where personal data are processed for direct marketing purposes, Camira shall recognise and respect the right of the data subject to object at any time to processing of personal data concerning the data subject for such marketing, which includes profiling to the extent that it is related to such direct marketing.

Where the data subject objects to processing for direct marketing purposes, Camira shall no longer be process the personal data for such purposes.

At the latest at the time of the first communication with the data subject, the right referred to in the first two paragraphs shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.

In the context of the use of information society services referenced earlier, and notwithstanding Directive 2002/58/EC, the data subject may exercise the data subject right to object by automated means using technical specifications.

Where personal data are processed for scientific or historical research purposes or statistical purposes, Camira shall recognise and respect the right of the data subject, on grounds relating to the data subject particular situation, to object to processing of personal data concerning the data subject, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

**Automated individual decision-making, including profiling**

Camira, in its capacity as a controller, shall recognise and respect the right of the data subject not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject.

The above paragraph shall not apply if the decision:

a. is necessary for entering into, or performance of, a contract between the data subject and Camira in its capacity as a controller;

b. is authorised by EU or domestic law to which Camira is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

c. is based on the data subject's explicit consent.

In the cases referred to in points (a) and (c) of the above paragraph, Camira shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of Camira to express the data subject point of view and to contest the decision.

Decisions referred to in the above paragraphs shall not be based on special categories of personal data referred to above unless the legal basis of explicit consent or substantial public interest as determined herein earlier applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

A decision is a "significant decision" for the purposes of this section if, in relation to a data subject, it:

a. produces legal effects concerning the data subject, or

b. similarly significantly affects the data subject.

A decision is a "qualifying significant decision" for the purposes of this section if:

a. it is a significant decision in relation to a data subject,

b. it is required or authorised by law, and

c. it does not fall within exceptions (a) and (c) above, that is decisions necessary to a contract or made with the data subject's consent.

Where Camira takes a qualifying significant decision in relation to a data subject based solely on automated processing:

a. Camira shall, as soon as reasonably practicable, notify the data subject in writing that a decision has been taken based solely on automated processing, and

b. the data subject may, before the end of the period of 21 days beginning with receipt of the notification, request Camira to:

i. reconsider the decision, or

ii. take a new decision that is not based solely on automated processing.

If such a request is made to Camira, then Camira shall, before the end of the period of 21 days beginning with receipt of the request:

a. consider the request, including any information provided by the data subject that is relevant to it;

b. comply with the request; and

c. by notice in writing inform the data subject of:

i. the steps taken to comply with the request, and

ii. the outcome of complying with the request.

# Restrictions

## Restrictions

Camira shall observe restrictions under EU or domestic law to which Camira is subject, by way of a legislative measure (including for example the UK Data Protection Act 2018) the scope of the obligations and rights provided for in the GDPR Articles 12 to 22 and GDPR Article 34, as well as the Principles set out in GDPR Article 5 in so far as its provisions correspond to the rights and obligations provided for in GDPR Articles 12 to 22, when such a restriction respects the essence of the fundamental rights and freedoms and is a necessary and proportionate measure in a democratic society to safeguards the interests identified at GDPR Article 23 and in particular, any legislative measure referred to in paragraph the above paragraph shall contain specific provisions at least, where relevant, as to those identified at GDPR Article 23.

# Controller and processor

## General obligations

### Responsibility of the controller

Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with currently applicable legislation. Those measures shall be reviewed and updated where necessary.

Where proportionate in relation to processing activities, the measures referred to in the above paragraph shall include the implementation of appropriate data protection policies, including this policy, by the controller.

Adherence to approved codes of conduct or approved certification mechanisms may be used as an element by which to demonstrate compliance with the obligations of the controller.

### Data protection by design and by default

Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing the controller, shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.

The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

An approved certification mechanism may be used as an element to demonstrate compliance with the requirements set out in the above paragraphs.

### Joint controllers

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

The joint controllers shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the 'information to be provided' referred to above, by means of an arrangement between controllers unless, and in so far as, the respective responsibilities of the controllers, are determined by EU or domestic law to which the controllers are subject. The arrangement may designate a contact point for data subjects.

The arrangement referred to in the above paragraph shall duly reflect the respective roles and relationships of the joint controllers vis-à-vis the data subjects. The essence of the arrangement shall be made available to the data subject.

Camira recognises that, irrespective of the terms of the arrangement referred to in the second paragraph, the data subject may exercise their rights under relevant legislation in respect of and against each of the controllers.

### Representatives of controllers or processors not established in the EU

Where processing of personal data of data subjects who are in the EU by a controller or processor not established in the EU, where the processing activities are related to:

a. the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the EU; or

b. the monitoring of their behaviour as far as their behaviour takes place within the EU;

the controller or the processor shall designate in writing a representative in the EU.

The obligation laid down in the first paragraph shall not apply to:

a. processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to above or processing of personal data relating to criminal convictions and offences referred to above, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

b. a public authority or body.

The representative shall be established in one of the EU Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

The representative shall be mandated by the controller or processor to be addressed in addition to or instead of of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with currently applicable legislation.

The designation of a representative by the controller or processor, shall be without prejudice to legal actions which could be initiated against the controller or the processor themselves.

**Processor**

Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the relevant compliance requirements and ensure the protection of the rights of the data subject.

The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

Processing by a processor shall be governed by a contract or other legal act under EU or domestic law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. That contract or other legal act shall stipulate, in particular, that the processor:

a. processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by EU or domestic law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest;

b. ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;

c. takes all measures required pursuant to the security of processing (as determined later herein);

d. respects the conditions referred to in the above paragraphs for engaging another processor;

e. taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III;

f. assists the controller in ensuring compliance with the controller's policies relating to security of processing, notification of a personal data breach to the supervisory authority, communication of a personal data breach to the data subject, data protection impact assessment and prior consultation, taking into account the nature of processing and the information available to the processor;

g. at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless EU or domestic law requires storage of the personal data;

h. makes available to the controller all information necessary to demonstrate compliance with this Policy, and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

With regard to point (h) above, the processor shall immediately inform the controller, if, in its opinion, an instruction infringes currently applicable data protection provisions.

Where a processor engages another processor for carrying out specific processing activities on behalf of the controller the same data protection obligations as set out in the contract or other legal act between the controller and the processor as referred to in the third paragraph shall be imposed on that other processor by way of a contract or other legal act under EU or domestic law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet currently applicable requirements. Where that other processor fails to fulfil its data protection obligations, the initial processor shall remain fully liable to the controller for the performance of that other processor's obligations.

Adherence of a processor to an approved code of conduct an approved certification mechanism may be used as an element by which to demonstrate sufficient guarantees as referred to in the first and fourth paragraphs.

Without prejudice to an individual contract between the controller and the processor, the contract or the other legal act referred to in the third and fourth paragraphs may be based, in whole or in part, on standard contractual clauses referred to in the seventh and eighth paragraphs, including when they are part of a certification granted to the controller or the processor.

The European Commission may lay down standard contractual clauses for the matters referred to in the third and fourth paragraphs and in accordance with its committee examination procedure.

A supervisory authority may adopt standard contractual clauses for the matters referred to third and fourth paragraphs in accordance with the European Commission's supervisory authority consistency mechanism.

The contract or the other legal act referred to in third and fourth paragraphs shall be in writing, including in electronic form.

Without prejudice to persons' rights to compensation and liability, and applicable administrative fines and penalties, if a processor infringes currently applicable legislation by determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing.

**Processing under the authority of the controller or processor**

The processor and any person acting under the authority of the controller, or of the processor, who has access to personal data, shall not process those data except on instructions from the controller unless required to do so by EU or domestic law.

**Records of processing activities**

Each controller, and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility.

That record shall contain all of the following information:

a. the name and contact details of the controller and, where applicable, the joint controller, the controller's

b. representative and the DPO, where applicable;

c. the purposes of the processing;

d. a description of the categories of data subjects and of the categories of personal data;

e. the categories of recipients to whom the personal data have been or will be disclosed including recipients in

f. third countries or international organisations;

g. where applicable, transfers of personal data to a third country or an international organisation, including the

h. identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of GDPR Article 49(1), the documentation of suitable safeguards;

i. where possible, the envisaged time limits for erasure of the different categories of data;

j. where possible, a general description of the technical and organisational security measures referred to herein later under Security of processing.

Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

a. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller, the processor's representative, and the DPO, where applicable;

b. the categories of processing carried out on behalf of each controller;

c. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of GDPR Article 49(1), the documentation of suitable safeguards;

d. where possible, a general description of the technical and organisational security measures referred to herein later at Security of processing.

The records referred to in the above paragraphs shall be in writing, including in electronic form.

The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.

The obligations on controllers and processors referred to in the first and second paragraphs above do not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data or personal data relating to criminal convictions and offences as referred to herein.

### Cooperation with the supervisory authority

The controller and the processor and, where applicable, their representatives, shall cooperate, on request, with the supervisory authority in the performance of its tasks.

## Security of personal data

### Security of processing

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, amongst other things, as appropriate:

a. the pseudonymisation and encryption of personal data;

b. the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

Camira shall implement such appropriate technical and organisational measures to ensure a level of security appropriate to the risk in accordance with its Information Security Policy.

Adherence to an approved code of conduct or an approved certification mechanism may be used as an element by which to demonstrate compliance with the requirements set out in the first paragraph.

The controller and the processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller unless the data subject is required to do so by EU or domestic law.

**Notification of a personal data breach to the supervisory authority**

In the case of a personal data breach, Camira, in its capacity as a controller, shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons, in accordance with its Data Breach Notification Procedures.

Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.

The processor shall notify Camira without undue delay after becoming aware of a personal data breach.

The notification referred to in the first paragraph shall at least:

a. describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

b. communicate the name and contact details of the DPO or other contact point where more information can be obtained;

c. describe the likely consequences of the personal data breach;

d. describe the measures taken or proposed to be taken by Camira to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

Camira shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with relevant requirements.

**Communication of a personal data breach to the data subject**

When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller, shall communicate the personal data breach to the data subject without undue delay.

Camira, its capacity as a controller, shall communicate the personal data breach to the data subject in accordance with its Data Breach Notification Procedures.

The communication to the data subject referred to in the above paragraph shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of the above section.

The communication to the data subject referred to in that paragraph shall not be required if any of the following conditions are met:

a. The controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

b. The controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in the first paragraph is no longer likely to materialise;

c. it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in the third paragraph are met.

## Data protection impact assessment and prior consultation

### Data protection impact assessment

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A single assessment may address a set of similar processing operations that present similar high risks.

The controller shall seek the advice of the DPO, where designated, when carrying out a data protection impact assessment (DPIA).

A DPIA referred to in the first paragraph shall in particular be required in the case of:

a. a systematic and extensive evaluation of personal aspects relating to natural persons which is based on

b. automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

c. processing on a large scale of special categories of as data defined above or of personal data relating to

d. criminal convictions and offences referred to earlier; or

e. a systematic monitoring of a publicly accessible area on a large scale.

f. Supervisory authorities shall establish and make public a list of the kind of processing operations which are subject to the requirement for a DPIA pursuant to the first paragraph, and may also establish and make public a list of the kind of processing operations for which no DPIA is required. Such lists shall be subject to the European Commission's supervisory authority consistency mechanism.

The DPIA assessment shall contain at least:

a. a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;

b. an assessment of the necessity and proportionality of the processing operations in relation to the purposes;

c. an assessment of the risks to the rights and freedoms of data subjects referred to in the first paragraph; and

d. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with relevant requirements taking into account the rights and legitimate interests of data subjects and other persons concerned.

Compliance with approved codes of conduct by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a DPIA.

Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Where processing on the legal basis of compliance or public interest as determined herein earlier has a legal basis in EU law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a DPIA has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, the above first seven paragraphs shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.

Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

**Prior consultation**

The controller shall consult the supervisory authority prior to processing where a DPIA indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

Where the supervisory authority is of the opinion that the intended processing referred to in the first paragraph would infringe the GDPR, in particular where the controller has insufficiently identified or mitigated the risk, the supervisory authority shall, within period of up to eight weeks of receipt of the request for consultation, provide written advice to the controller and, where applicable to the processor, and may use any of its powers.

That period may be extended by six weeks, taking into account the complexity of the intended processing.

The supervisory authority shall inform the controller and, where applicable, the processor, of any such extension within one month of receipt of the request for consultation together with the reasons for the delay.

Those periods may be suspended until the supervisory authority has obtained information it has requested for the purposes of the consultation.

When consulting the supervisory authority pursuant to the first paragraph, the controller shall provide the supervisory authority with:

a. where applicable, the respective responsibilities of the controller, joint controllers and processors involved in the processing, in particular for processing within a group of undertakings;

b. the purposes and means of the intended processing;

c. the measures and safeguards provided to protect the rights and freedoms of data subjects pursuant to the

d. relevant legislation;

e. where applicable, the contact details of the DPO;

f. the data protection impact assessment; and

g. any other information requested by the supervisory authority.

Member States are required to consult the supervisory authority during the preparation of a proposal for a legislative measure to be adopted by Parliament, or of a regulatory measure based on such a legislative measure, which relates to processing.

Notwithstanding the first paragraph, Member State law may require controllers to consult with, and obtain prior authorisation from, the supervisory authority in relation to processing by a controller for the performance of a task carried out by the controller in the public interest, including processing in relation to social protection and public health.

## Data protection officer

### Designation of the DPO

The controller and the processor are required to designate a Data Protection Officer (DPO) in any case where:

a. the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

b. the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

c. the core activities of the controller or the processor consist of processing on a large scale of special categories of data and personal data relating to criminal convictions and offences referred to earlier.

A group of undertakings may appoint a single DPO provided that a DPO is easily accessible from each establishment.

Where the controller, or the processor is a public authority or body, a single DPO may be designated for several such authorities or bodies, taking account of their organisational structure and size.

In cases other than those referred to in the first paragraph, the controller, or processor or associations and other bodies representing categories of controllers or processors may or, where required by EU or domestic law shall, designate a DPO. The DPO may act for such associations and other bodies representing controllers or processors.

The DPO shall be designated on the basis of professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfil the tasks referred to below.

The DPO may be a staff member of the controller, or processor, or fulfil the tasks on the basis of a service contract.

The controller or the processor shall publish the contact details of the DPO and communicate them to the supervisory authority.

**Determination of designation of the DPO**

With reference to WP29 guidelines, definitions and recommendations, Camira determines that mandatory designation of Data Protection Officer is not applicable to Camira.

When a DPO is designated a DPO on a voluntary basis, the same requirements apply to the designation, position and tasks as if the designation had been mandatory.

Camira therefore further determines that it shall not designate a DPO on a voluntary basis.

Camira may employ staff and/or outside consultants with tasks relating to the protection of personal data.

In so doing, Camira shall ensure that there is no confusion regarding their title, status, position and tasks and shall make clear, in any communications within the company, as well as with data protection authorities, data subjects, and the public at large, that the title of this individual or consultant is not a 'DPO'.

In accordance with and with reference to WP29 guidelines, definitions and recommendations, Camira documents as follows the internal analysis carried out to determine whether or not a DPO is to be appointed in order to be able to demonstrate that the relevant factors have been taken into account properly:

Processing in the context of Camira's activities is not carried out by a public authority or body, therefore mandatory designation of a DPO pursuant to requirement (a) is not applicable to Camira.

The core activities of Camira do not consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale (by any definition), therefore mandatory designation of a DPO pursuant to requirement (b) is not applicable to Camira.

The core activities of the Camira do not consist of processing on a large scale (by any definition) of special categories of data and personal data relating to criminal convictions and offences referred to earlier, therefore mandatory designation of a DPO pursuant to requirement (C) is not applicable to Camira.

**Position of the DPO**

1. The controller and the processor shall ensure that the DPO is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
2. The controller, and processor shall support the DPO in performing the tasks referred to below by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain the data subject expert knowledge.

The controller and processor shall ensure that the DPO does not receive any instructions regarding the exercise of those tasks. The data subject shall not be dismissed or penalised by the controller or the processor for performing his tasks.

The DPO shall directly report to the highest management level of the controller or a processor.

Data subjects may contact the DPO with regard to all issues related to processing of their personal data and to the exercise of their rights under relevant legislation.

The DPO shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with EU or domestic law.

The DPO may fulfil other tasks and duties.

Camira shall ensure that any such tasks and duties do not result in a conflict of interests.

Conflict of interests may arise, for example, where the DPO determines the purposes and the means of the processing of personal data and/or where the DPO manages competing objectives that could result in data protection taking a secondary role to business interests.

**Tasks of the DPO**

The DPO shall have at least the following tasks:

a. to inform and advise Camira or the processor and the employees who carry out processing of their obligations pursuant to relevant data protection provisions;

b. to monitor compliance with relevant data protection provisions and with the policies of Camira or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

c. to provide advice where requested as regards the DPIA and monitor its performance pursuant to Camira's policies relating to DPIAs referred to earlier;

d. to cooperate with the supervisory authority;

e. to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to earlier, and to consult, where appropriate, with regard to any other matter.

The DPO shall in the performance of the data subject tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

## Codes of conduct and certification

Any certifications, claims of conformance and adherence to codes of conduct held by a controller or processor do not reduce the responsibility of the controller or the processor for compliance with applicable legislation.

# Transfers of personal data to third countries or international organisations

## General principle for transfers

Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to relevant compliance requirements are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation.

All provisions herein shall be applied in order to ensure that the level of protection of natural persons guaranteed by relevant legislation is not undermined.

## Transfers on the basis of an adequacy decision

The European Commission is required to publish in the Official Journal of the European EU, and on its website, a list of the third countries, territories and specified sectors within a third country and international organisations for which it has decided that an adequate level of protection is or is no longer ensured.

A transfer of personal data to a third country or an international organisation may only take place without a requirement for any specific authorisation where the European Commission has published an adequacy decision that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection.

## Transfers subject to appropriate safeguards

In the absence of a published adequacy decision, a controller or processor may transfer personal data to a third country or an international organisation only if the controller, or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.

The appropriate safeguards referred to in the first paragraph may be provided for, without requiring any specific authorisation from a supervisory authority, by:

a. a legally binding and enforceable instrument between public authorities or bodies;

b. binding corporate rules in accordance with the provisions set out below;

c. standard data protection clauses adopted by the European Commission in accordance with its committee examination procedure;

d. standard data protection clauses adopted by a supervisory authority and approved by the European Commission in accordance with its committee examination procedure;

e. an approved code of conduct together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights; or

f. an approved certification mechanism together with binding and enforceable commitments of the controller or processor in the third country to apply the appropriate safeguards, including as regards data subjects' rights.

Subject to the authorisation from the competent supervisory authority, the appropriate safeguards referred to in the first paragraph may also be provided for, in particular, by:

a. contractual clauses between the controller, or processor and the controller, processor or the recipient of the personal data in the third country or international organisation; or

b. provisions to be inserted into administrative arrangements between public authorities or bodies which include enforceable and effective data subject rights.

## Binding corporate rules

The competent supervisory authority shall approve binding corporate rules in accordance with the European Commission's supervisory authority consistency mechanism, provided that they:

a. are legally binding and apply to and are enforced by every member concerned of the group of undertakings, or group of enterprises engaged in a joint economic activity, including their employees;

b. expressly confer enforceable rights on data subjects with regard to the processing of their personal data; and

c. fulfil the requirements laid down in the second paragraph.

The binding corporate rules referred to in the first paragraph shall specify at least:

a. the structure and contact details of the group of undertakings, or group of enterprises engaged in a joint economic activity and of each of its members;

b. the data transfers or set of transfers, including the categories of personal data, the type of processing and its purposes, the type of data subjects affected and the identification of the third country or countries in question;

c. their legally binding nature, both internally and externally;

d. the application of the general data protection principles, in particular purpose limitation, data minimisation, limited storage periods, data quality, data protection by design and by default, legal basis for processing, processing of special categories of personal data, measures to ensure data security, and the requirements in respect of onward transfers to bodies not bound by the binding corporate rules;

e. the rights of data subjects in regard to processing and the means to exercise those rights, including the right not to be subject to decisions based solely on automated processing, including profiling, the right to lodge a complaint with the competent supervisory authority and before the competent courts of the Member States in accordance with data subjects' rights to an effective judicial remedy against a controller or processor, and to obtain redress and, where appropriate, compensation for a breach of the binding corporate rules;

f. the acceptance by the controller or processor established on the territory of the United Kingdom of liability for any breaches of the binding corporate rules by any member concerned not established in the EU; the controller or the processor shall be exempt from that liability, in whole or in part, only if it proves that that member is not responsible for the event giving rise to the damage;

g. how the information on the binding corporate rules, in particular on the provisions referred to in points (d), (e) and (f) of this paragraph is provided to the data subjects in addition to information to be provided where personal data are collected from the data subject or otherwise;

h. the tasks of any DPO designated in accordance with the controller's policy relating to the designation of the DPO determined herein earlier or any other person or entity in charge of the monitoring compliance with the binding corporate rules within the group of undertakings, or group of enterprises engaged in a joint economic activity, as well as monitoring training and complaint-handling;

i. the complaint procedures;

j. the mechanisms within the group of undertakings, or group of enterprises engaged in a joint economic activity for ensuring the verification of compliance with the binding corporate rules. Such mechanisms shall include data protection audits and methods for ensuring corrective actions to protect the rights of the data subject. Results of such verification should be communicated to the person or entity referred to in point (h) and to the board of the controlling undertaking of a group of undertakings, or of the group of enterprises engaged in a joint economic activity, and should be available upon request to the competent supervisory authority;

k. the mechanisms for reporting and recording changes to the rules and reporting those changes to the supervisory authority;

l. the cooperation mechanism with the supervisory authority to ensure compliance by any member of the group of undertakings, or group of enterprises engaged in a joint economic activity, in particular by making available to the supervisory authority the results of verifications of the measures referred to in point (j);

m. the mechanisms for reporting to the competent supervisory authority any legal requirements to which a member of the group of undertakings, or group of enterprises engaged in a joint economic activity is subject in a third country which are likely to have a substantial adverse effect on the guarantees provided by the binding corporate rules; and

n. the appropriate data protection training to personnel having permanent or regular access to personal data.

The Commission may specify the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules within the meaning of this Policy. Those implementing acts shall be adopted in accordance with its committee examination procedure.

## Transfers or disclosures not authorised by EU law

Any judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the EU or the United Kingdom, without prejudice to other grounds for transfer pursuant to this chapter.

## Derogations for specific situations

In the absence of an adequacy decision, or of appropriate safeguards, including binding corporate rules, a transfer or a set of transfers of personal data to a third country or an international organisation shall take place only on one of the following conditions:

a. the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;

b. the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;

c. the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;

d. the transfer is necessary for important reasons of public interest;

e. the transfer is necessary for the establishment, exercise or defence of legal claims;

f. the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent;

g. the transfer is made from a register which according to EU or domestic law is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by EU or domestic law for consultation are fulfilled in the particular case.

Where a transfer could not be based on an adequacy decision, or of appropriate safeguards, including the provisions on binding corporate rules, and none of the derogations for a specific situation referred to in the first subparagraph of this paragraph is applicable, a transfer to a third country or an international organisation may take place only if the transfer is not repetitive, concerns only a limited number of data subjects, is necessary for the purposes of compelling legitimate interests pursued by The controller which are not overridden by the interests or rights and freedoms of the data subject, and The controller has assessed all the circumstances surrounding the data transfer and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data. The controller shall inform the supervisory authority of the transfer. The controller shall, in addition to providing the information to be provided where personal data are collected from the data subject or otherwise, inform the data subject of the transfer and on the compelling legitimate interests pursued.

A transfer pursuant to point (g) of the first subparagraph of the first paragraph shall not involve the entirety of the personal data or entire categories of the personal data contained in the register. Where the register is intended for consultation by persons having a legitimate interest, the transfer shall be made only at the request of those persons or if they are to be the recipients.

Points (a), (b) and (c) of the first subparagraph of the first paragraph and the second subparagraph thereof shall not apply to activities carried out by public authorities in the exercise of their public powers.

The public interest referred to in point (d) of the first subparagraph of the first paragraph shall be recognised in EU law or in the law of the Member State to which The controller is subject.

In the absence of an adequacy decision, EU or domestic law may, for important reasons of public interest, expressly set limits to the transfer of specific categories of personal data to a third country or an international organisation. Member States shall notify such provisions to the Commission.

The controller, or processor shall document the assessment as well as the suitable safeguards referred to in the second subparagraph of the first paragraph in records referred to herein under Records of processing activities.

A Croall

....................................................

ANTHONY CROALL

Commercial Director
Dated: December 2019